Information Assurance (IA): A Different View

Mario Balakgie
Chief Information Assurance Officer
Defense Intelligence Agency

18 April 2000

Form SF298 Citation Data

Report Date *("DD MON YYYY")* 18042000	**Report Type** N/A	**Dates Covered (from... to)** *("DD MON YYYY")*

Title and Subtitle Information Assurance (IA):A Different View	**Contract or Grant Number**
	Program Element Number
Authors Balakgie, Mario	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) Defense Intelligence Agency	**Performing Organization Number(s)**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Monitoring Agency Acronym**
	Monitoring Agency Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract	
Subject Terms	
Document Classification unclassified	**Classification of SF298** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** unlimited
Number of Pages 22	

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	4/18/00	Briefing

4. TITLE AND SUBTITLE
IA: A Different View

5. FUNDING NUMBERS

6. AUTHOR(S)
Mario Balakgie

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

IATAC
Information Assurance Technology Analysis
Center
3190 Fairview Park Drive
Falls Church VA 22042

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center
DTIC-IA
8725 John J. Kingman Rd, Suite 944
Ft. Belvoir, VA 22060

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

This DIA briefing discusses Information Assurance from a different point of view. It first defines information superiority centered on the network and then looks at the opportunities in this area. It discusses the operations, people, threat, the policy and the technology.

14. SUBJECT TERMS
Information Assurance, Security,

15. NUMBER OF PAGES

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	UNCLASSIFIED	UNCLASSIFIED	None

Information Superiority

- Introduces concept of Network Centric Warfare
- Network Power is Combat Power
- Network Defense is Combat Power Protection
- Our information systems strength can become a critical vulnerability

Opportunities

- IT is key to operations
  - Warfighter is dependent
  - Networks must be reliable

- People are critical
  - Trained and experienced
  - Retained and satisfied

- Policy leads integration
  - Standards
  - Responsibilities
  - Direction

- Threats are real
  - Explosion in access
  - More to protect

- Technology must integrate security
  - Computing and connectivity
  - Software
  - User interface and access

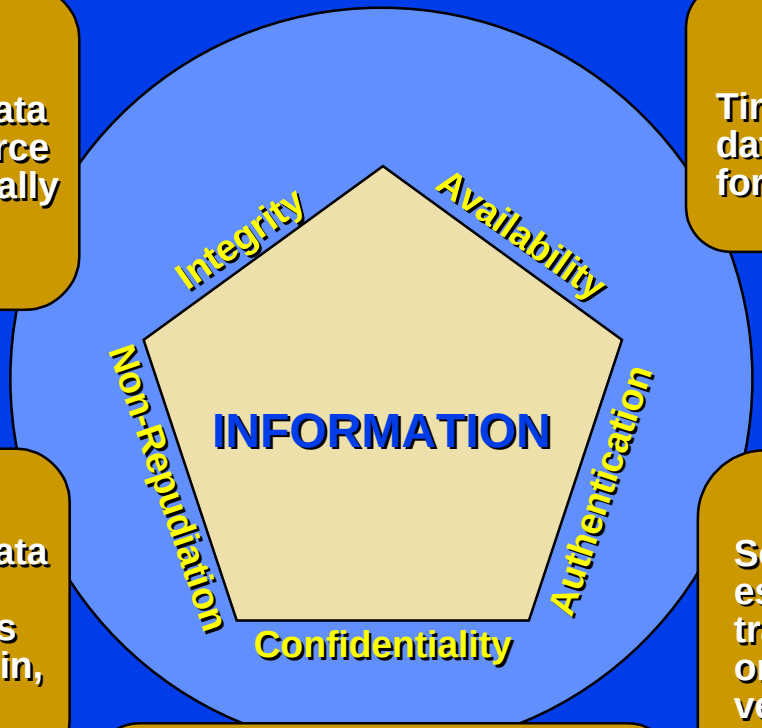
Elements of IA

INTEGRITY

Condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.

AVAILABILITY

Timely, reliable access to data and information services for authorized users.



NON-REPUDIATION

Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of origin, so neither can later deny having processed the data.

AUTHENTICATION

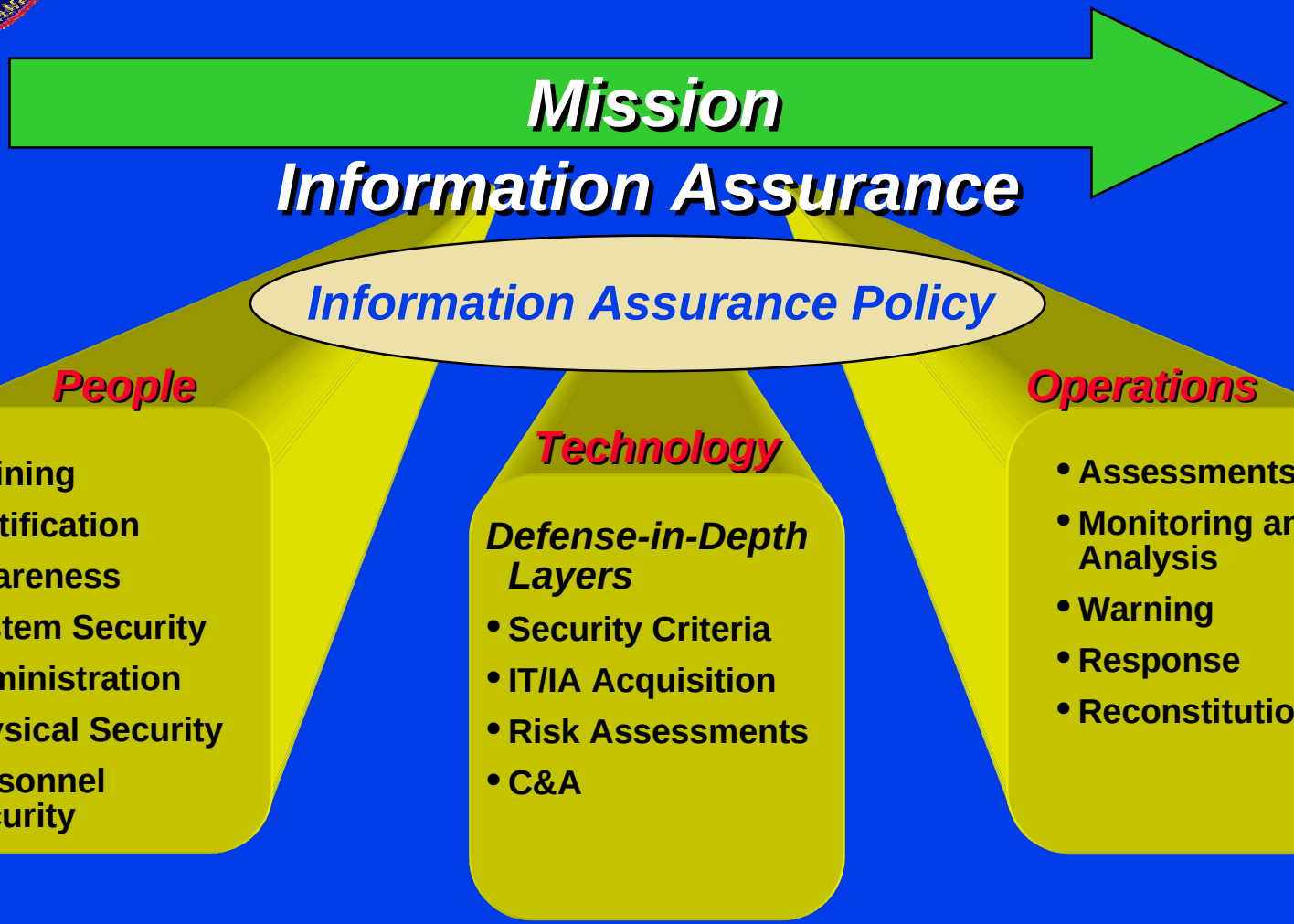
Security measure designed to establish the validity of a transmission, message, user, or system or a means of verifying an individual's authorization to receive specific categories of information.

CONFIDENTIALITY

Assurance that information is not disclosed to unauthorized persons, processes, or devices.

* Source DIAP

Multidimensional Approach



* Source DIAP

Nature of the Business (Problem)

- Dynamic environment
- Multiple points of security failures
- Vulnerabilities occur unexpectedly
- Only as strong as the weakest link
- Problem goes beyond the IA professionals

What Needs to be Done?

- Must be enterprise-wide strategy
- Require risk management business practice
- Ensure SCI Infrastructure is reliable and secure
- Priority commitment
- Protect all networks; all classification
- Focus on the human element
- Implement Defense-in-Depth

How do we get there?

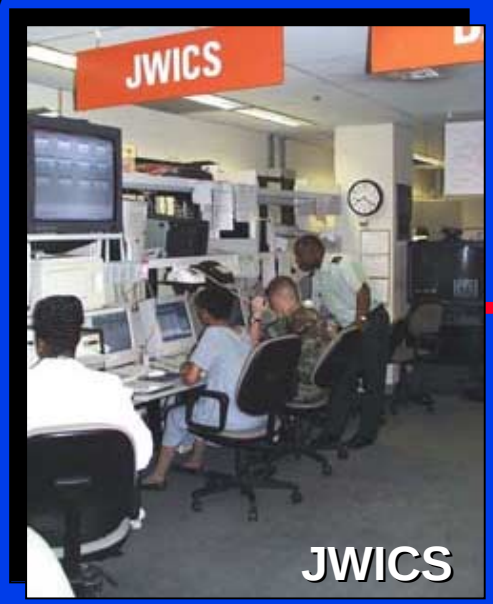
Defense-in-Depth

- Protect the network
- Protect the enclave
- Protect the computing environment
- Public key infrastructure
- Detect and respond

Strategic Partnership

Protect the Network

- Confidentiality
- Availability
- Integrity



Network Operations Center

- Network Management
- Visibility
- Encryption (Type 1)
- Router-to-Router

Switches/Router Management and Security

Local Network Operations

Site Infrastructure (DoDIIS and non-DoDIIS)

Enterprise Infrastructure Protection

- Security Services

Protect the Enclave

Router Filtering

Firewall

Site Infrastructure (SCI) (DoDIIS and non-DoDIIS)

Enterprise Infrastructure Protection

Non-SCI

Approved Controlled Interface (Guard)

Unclassified

Network Operations Center

- Intrusion Detection
- INFOCON Alert
- Enterprise-wide assessment of controlled interface
- Re-validate req for controlled interface
- Reduce numbers
- Concentrate on approved list

Protecting the Computing Environment

- Access Management
- Audits
- Intrusion detection
- Virus protection
- Configuration Management
- Operation System Security
- PKI applications
- Vulnerability assessments

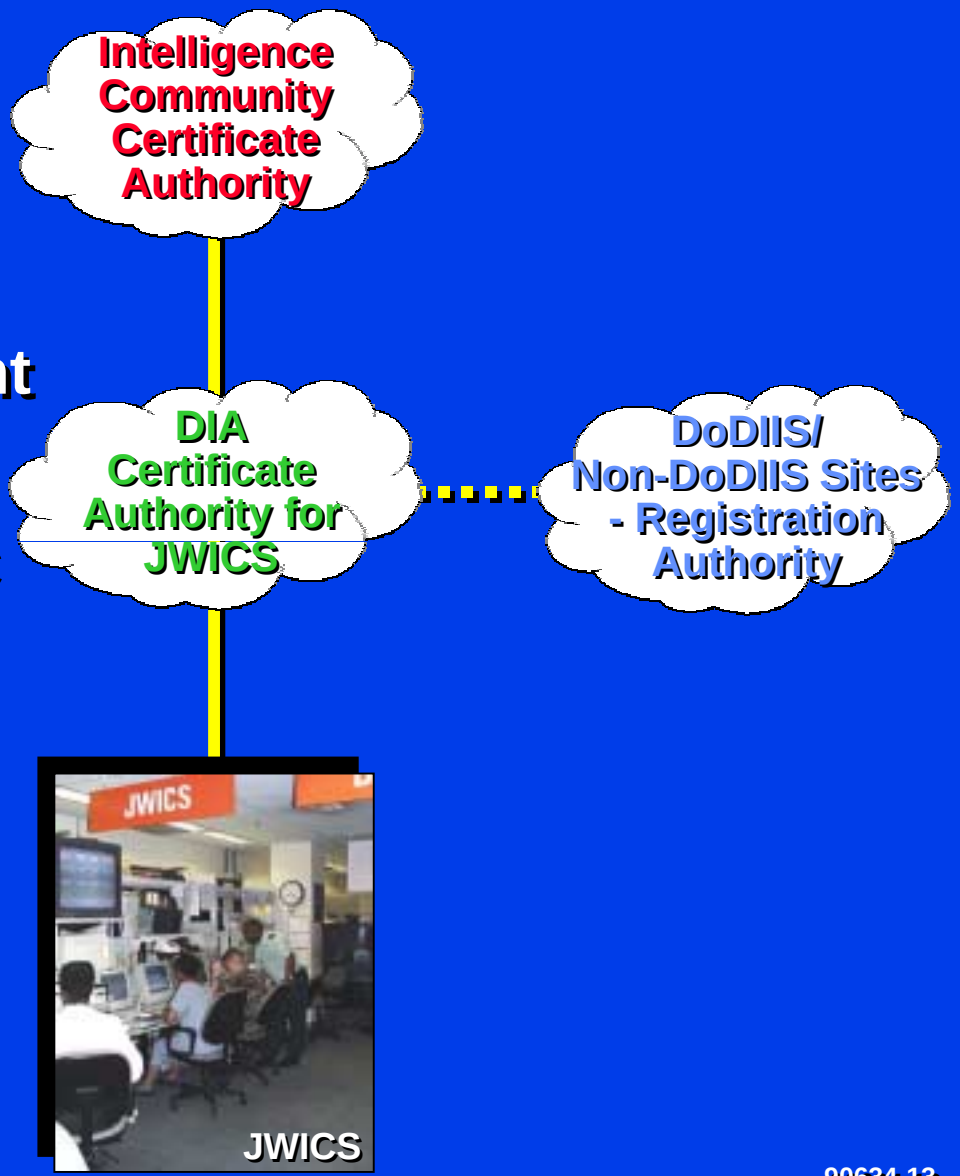
User Workstation

Servers
Web application
Mission application

- Information System Security Management critical to success
- Chief Information Officer role
- Protection against the insider
- Manage and license system administrators

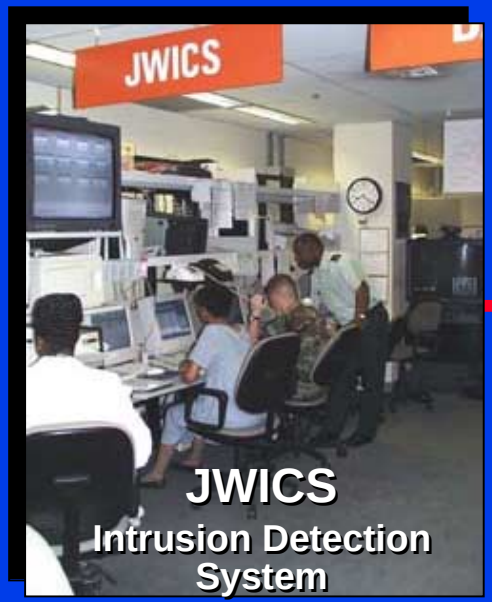
Public Key Infrastructure

- Enterprise-wide management
- Operations emphasis
- Single approach DoD and IC
- Design and architecture being evaluated
- DMB action item



Detect & Respond

- Monitor
- Analyze
- Respond
- Report



JWICS
Intrusion Detection System

Network Operations Center

- Monitoring
- Computer Network Defense (CND)
- Enterprise-wide management

Site Infrastructure (DoDIIS and non-DoDIIS)

- Internal Intrusion Detection System Report (CND)

Initiatives

- **Development of DODIIS IA Strategy**
  - **Coordinate with DMB**
- **Modeling an IA business process & risk management practice**
  - **Automated tool**

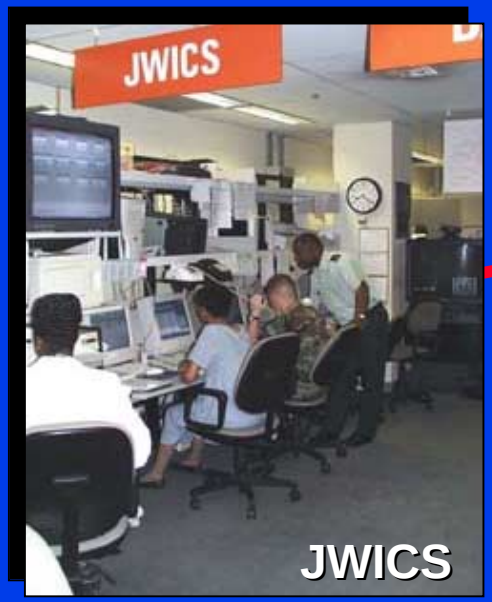
Conclusion

- Enterprise wide IA management is essential
- Apply disciplined business process
- Risk management practice required
- New growth area with demanding environment

The Face of IA

Questions and Comments

Protect the Enclave



Network Operations Center

- Intrusion Detection
- INFOCON Alert

Router Filtering

Firewalls

Site Infrastructure (SCI) (DoDIIS and non-DoDIIS)

Approved Controlled Interface (Guard)

Non-SCI

Unclassified

- Enterprise-wide assessment of controlled interface
- Re-validate req for controlled interface
- Reduce numbers
- Concentrate on approved list

Big IA Brother is Watching You!

Mission

- The primary function of IA is to advise the decisionmaker of risks by assessing and recommending methods to reduce those risks to the information infrastructure

Institutionalize Business and Risk Management Processes